REMARKS

Claims 4, 21 and 27 have been canceled above. Claims 2, 5-7 and 9-15 were previously canceled. Claims 31-39 have been added.

Claim 1, 3, 8 and 16-20, 22-26 and 28-30 are pending, were rejected under 35 USC 112, second paragraph, and have been corrected above.

Claims 1, 3, 8 and 16-20, 22-26 and 28-30 were rejected under 35 USC 103 based on "Virtualizing I/O Devices on VMware Workstation's Hosted Virtual Machine Monitor" ("VMware") and Bornstein et al. Applicants respectfully traverse this rejection based on the following:

Amended 1 recites a method for communicating from a first virtual machine to an external device. A base portion of a virtual machine operating system forms the first virtual machine and other virtual machines from a CPU, storage and other real resources of a real computer by respective allocations of the CPU, storage and other real resources to the first virtual machine and the other virtual machines. The base portion controls all of the virtual machines and provides communication pathways for communications from the first virtual machine to the other virtual machines and to a tangible network adapter card coupled to an external network leading to the external device. The first virtual machine writes an IP datagram to an output buffer within storage allocated to the first virtual machine. The IP datagram comprises data and a destination IP address associated with the external device. The base portion copies the IP datagram from the output buffer into storage allocated to the base portion such that the IP datagram passes from the first virtual machine into the storage of the base portion without passing through any other virtual machines. The base portion identifies the destination IP address from the IP datagram and determines from a list of IP addresses for other virtual machines that the destination IP address does not correspond to any of the other virtual machines in the real computer. In response, the base portion forwards the IP datagram, addressed to the destination IP address, to the tangible network adapter card. The tangible

network adapter card sends the IP datagram to the destination IP address via the external network.

Thus, amended claim 1 recites that the base portion forms the virtual machines from a CPU, storage and other real resources of the computer, controls all of the virtual machines and provides a communication pathway between the first virtual machine and the other virtual machines. The base portion identifies the destination IP address from the IP datagram and determines from the list of IP address for other virtual machines in the real computer that the destination IP address does not correspond to any of the other virtual machines in the real computer. In response, the base portion forwards the IP datagram, addressed to the destination address, to a tangible network adapter card coupled to an external network leading to the external device.

There are at least two key differences between VMware and amended claim 1. First, amended claim 1 recites communications based on IP addresses which is layer 3 in the OSA model. In contrast, VMware discloses communications based on MAC addresses which is layer 2 in the OSA model. "The virtual NIC appears to the guest as a full-fledged PCI Ethernet controller, complete with its own MAC address. ... A virtual NCI that is bridged to a physical NIC is a true Ethernet bridge in the strictest sense. Its packets are sent on the wire with its own unique MAC address." VMware Section 2.2 first and second paragraphs. MAC addresses are used for layer 2 communications, in contrast to claim 1. Second, as illustrated in Figure 3 of VMware, VMware teaches a separate Virtual Machine Monitor ("VMM") for each virtual machine. The VMM defines the virtual machines, "In this architecture, the CPU virtualization is handled by the VMM." VMware section 2 third paragraph. There is not one VMM of VMware that controls all the virtual machines in contrast to the base portion recited in amended claim 1. In fact, each VMM of VMware is dedicated to a respective virtual machine. Moreover, because "CPU virtualization is handled by the VMM" in VMware and there is a separate instance of VMM for each virtual machine, the host operating system of VMware does not form the virtual machines or allocates resources for the virtual machines as does the base portion recited in claim 1. Therefore, the host operating system of VMware does not correspond to the base portion of claim 1, as asserted by the Examiner. It should also be noted that the "virtual machine monitor

component (VMM) runs directly on the hardware", so the function of each VMM does not involve the host operating system of VMware. See VMware section 2 second paragraph.

Bornstein discloses:

> "Upon receipt of the first message from the external device 22, the network address translation module 44 reads the first address 74 and translates the first address to a second address 82. The second address becomes part of the header 80 of the second message 81. In one embodiment of the invention, communication of the second message 81 involves replacing the first address 74 field in the first message 71 with the second address 82. In a different embodiment of the invention, the header 72 and data 73 components of the first message 71 are first separated from one another, a header 80 is created for the second message 81 including the second address 82, then Th. header 80 of the second message 81 and the data 76 are combined to create a new message 58 or 62.
>
> It should be noted that standard IP packets are suitable for sue as the first message 71, 81. In particular, the first and second addressees 74, 82 can be source addressees of the IP packets, and the port identifier 75, 77 can be the port identifiers of the IP packets.
>
> FIG. 4 is a table 84 suitable for use in translation a first message 34 to a second message 58, 62. The table includes a column of port identifiers 85 and a column of internal destination addressees 86. Upon receipt of the first message 71 containing a first address 74, (designating the data communications device 40), the network translation module 44 conducts a translation 78. Accordingly, the network address translation module 44 locates a port identifier value from the table port column 85 equivalent to the port identifier value from the table port column 85 equivalent to the port identifier 75 that appears in the first message 71. The network translation module 44 then selects the second address 82 corresponding to the located port identifier row in the internal destination address column 86 and uses that as the second address 82 of the second message 81." Column 7 lines 9-40.

It would not have been obvious to combine VMware with Bornstein et al. because VMware pertains to OSA model layer 2 communications (i.e. communications based on MAC addresses) whereas Bornstein et al. pertain to OSA model layer 3 communications (i.e. communications based on IP address). To support the combination of VMware with an OSA layer 3 document, the Examiner cites one sentence of VMware which states "If desired, the host OS can perform routing or IP masquerading to connect a virtual network to any type of external network, even to a non-Ethernet network." This is a cryptic sentence whose meaning and implementation are nebulous; it is not clear what "IP masquerading" means. It is not even known if this involves OSA model layer 3 communications or a substitute. Moreover, this is not the part of VMware that the Examiner attempts to combine with Bornstein et al. Therefore, it was not proper to combine VMware with Bornstein et al.

Also, in contrast to claim 1, Bornstein et al. require translation of the destination address of all IP datagrams received from an external network or from another virtual machine in the same real machine. "Upon receipt of the first message 71 from the external device 22, the network address translation module 44 reads the first address 74 and translates the first address 74 to a second address 82." Bornstein et al. Column 7 lines 9-11. "It is also possible for communications to exist between the two virtual machines 100 and 106. In order to do so, one virtual machine, virtual machine 100, for example, sends a message 116 to the translation process 104. Upon receipt by the translation process 104, the message 116 is translated in the same manner as translation performed for a first message 34 received from an external device 22 as described in FIGS. 1-3. After translation, the message 118 is transmitted to the other virtual machine 106." Bornstein et al. Column 9 lines 32-39. Thus, Bornstein et al. translate the destination address of all IP datagrams received from an external network or from another virtual machine in the same real machine. According to the present invention, as recited in claim 1, a virtual machine in a real computer uses the destination IP addresses provided by the originating virtual machine to address external devices as well as other virtual machines in the same real computer, so there is no address translation. Therefore, Bornstein et al. teach away from the present invention.

Moreover, in contrast to claim 1, Bornstein et al. do not teach or suggest how a virtual machine can **send** an IP datagram **to** an external network. Bornstein et al. only teach how a virtual machine can **receive** an IP datagram **from** an external network or **from** another virtual machine in the same real machine. The table 84 of Bornstein et al. is only used for correlating a port 85 **to an Internal Destination address 86**. Therefore, the table 84 of Bornstein et al. cannot be used to identify the IP address of an external device for outgoing IP datagrams. Therefore, Bornstein et al. do not teach or suggest the features of claim 1 which enable a virtual machine to send an IP datagram to an external network.

Also, it would not have been obvious in view of Bornstein et al. to modify VMware to handle layer 3/IP communications because a destination IP address in a layer 3 IP communication is more difficult to uncover than a MAC address in a layer 2 communication. Such a modification would require the VMNet Driver of VMware to uncover and read the destination IP address in every IP datagram. Moreover, VMware pertains to layer 2 communications and therefore, do not suggest modification of a layer 3 IP communication according to claim 1.

Claims 3, 8, 16-18 and 31-33 depend on claim 1 and therefore, distinguish over the prior art for the same reasons that claim 1 distinguishes thereover.

Independent claim 19 distinguishes over the prior art for the same reasons that independent claim 1 distinguishes thereover. Claims 20, 22-24 and 34-36 depend on claim 19.

Independent claim 25 distinguishes over the prior art for the same reasons that independent claim 1 distinguishes thereover. Claims 26, 28-29 and 37-39 depend on claim 25.

In addition, claim 32 recites that the base portion forwards the IP datagram to the tangible network adapter card without translation of the destination IP address in the IP datagram as written by the first virtual machine to the output buffer within the storage allocated to the first virtual machine. This clearly distinguishes over Bornstein et al. which requires translation of all

addresses and therefore teaches away from the present invention. Claims 35 and 38 similarly distinguish over Bornstein et al.

In addition, claim 33 recites that the base portion copies the second IP datagram into the input buffer within the storage allocated to the second virtual machine without translation of the destination IP address in the second IP datagram as written by the first virtual machine to the second output buffer within the storage allocated to the first virtual machine. This clearly distinguishes over Bornstein et al. which requires translation of all addresses and therefore teaches away from the present invention. Claims 36 and 39 similarly distinguish over Bornstein et al.

Based on the foregoing, Applicant requests allowance of the present patent application as amended above.

Respectfully submitted,

Dated: 09/05/07 /Arthur J. Samodovitz/
Telephone: 607-429-4368 Arthur J. Samodovitz
Fax No.: 607-429-4119 Reg. No. 31,297